(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 October 2003 (09.10.2003)

PCT

(10) International Publication Number
WO 03/084166 A1

(51) International Patent Classification[7]: H04L 29/06, 9/08

(21) International Application Number: PCT/GB03/01096

(22) International Filing Date: 14 March 2003 (14.03.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
02252215.5 27 March 2002 (27.03.2002) EP
02252217.1 27 March 2002 (27.03.2002) EP

(71) Applicant *(for all designated States except US)*: **BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY** [GB/GB]; 81 Newgate Street, London EC1A 7AJ (GB).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **SOPPERA, Andrea** [IT/GB]; 21 Almondayes, IPSWICH, Suffolk IP2 9SH (GB).

(74) Agent: **WALLIN, Nicholas, James**; BT Group Legal, Intellectual Property Department, Holborn Centre, 8th Floor, 120 Holborn (GB).

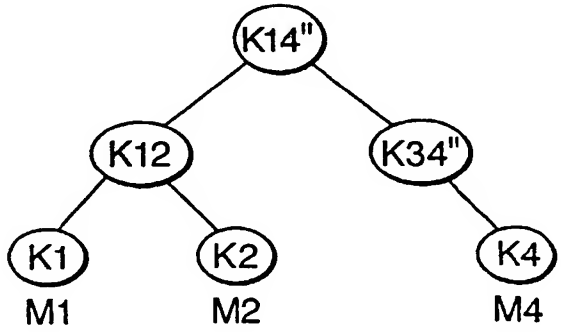
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Published:**
— *with international search report*

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

(54) Title: KEY MANAGEMENT PROTOCOL




(57) Abstract: A key distribution server maintains a tree of nodes. Members of a group who are allowed access to information are associated with respective leaf nodes of the tree. The information is encrypted with a key comprising a join key field and a leave field, and these are associated with the root node of the tree. The join key is updated each time a member joins the group and the leave field is updated each time a member leaves. Further respective leave keys are associated with the other nodes of the tree. The leave keys of the tree are related so that a member knowing the leave key of its node can work out the leave key of the root node and hence decrypt the information. The key distribution server transmits offset messages to the members to allow them so to calculate the root node leave key. The system of offset messages reduces the amount of communication required between the key distribution server and the group members.

WO 03/084166 A1